CSC-EPL-89/006

(2)

NATIONAL COMPUTER SECURITY CENTER

FINAL EVALUATION REPORT

OF

ALC Incorporated

TIGERSAFE

1 October 1989

Approved for Public Release:
Distribution Unlimited

FINAL EVALUATION REPORT

ALC Incorporated

Tigersafe

NATIONAL

COMPUTER SECURITY CENTER

9800 Savage Road
Fort George G. Meade
Maryland 20755-6000

1 October 1989

CSC-EPL-SUM-89/006
Library No. S235,425

FOREWORD

This publication, the Final Evaluation Report ALC Tigersafe is being issued by the National Computer Security Center under the authority of and in accordance with DoD Directive 5215.1, "Computer Security Evaluation Center." The purpose of this report is to document the results of the ALC evaluation. The requirements stated in this report are taken from the *Computer Security Subsystem Interpretation* of the *Department of Defense Trusted Computer System Evaluation Criteria* dated 16 September 1988.

Approved:

Patrick R. Gallagher, Jr.
National Security Agency /
National Computer Security Center

1 October 1989

ACKNOWLEDGEMENTS

Team Members

Team members included the following individuals, who were provided by the following organization:

Diann A. Carpenter
Capt. Steve Schneider, USA

National Security Agency
Trusted Product and Network Security Evaluation Division
9800 Savage Road
Fort George G. Meade, Maryland 20755-6000

For their contributions to this evaluation, acknowledgement is given to Capt. Benton Wigney USAF, Michael Oehler, Walt Roddy, and 1Lt. Reggie Sharpless USAF.

Contents

FOREWORD i

ACKNOWLEDGEMENTS ii

EXECUTIVE SUMMARY v

Chapter 1 Introduction 1
- Evaluation Process Background . . . 1
- Subsystem Evaluation Program . . . 2
- Document Organization . . . 2

Chapter 2 System Overview 4
- Product History . . . 4
- Product Overview . . . 4
- Security Relevant Portion (SRP) . . . 5
  - Hardware Architecture . . . 5
  - Software Architecture . . . 6
  - Tigersafe Utilities . . . 7
- SRP Protected Resources . . . 9
  - Subjects . . . 9
  - Objects . . . 9
- SRP Protection Mechanisms . . . 10
  - Identification and Authentication . . . 10
  - Object Reuse . . . 11

Chapter 3 Evaluation as a Subsystem 12
- Features . . . 12
  - Identification and Authentication . . . 12
  - Object Reuse . . . 14
- Assurances . . . 15
  - System Architecture . . . 15
  - System Integrity . . . 16
  - Security Testing . . . 17
- Documentation . . . 18
  - Security Features User's Guide . . . 18
  - Trusted Facility Manual . . . 19
  - Test Documentation . . . 20
  - Design Documentation . . . 21
- Rating Assignment . . . 22

Chapter 4 Evaluator's Comments **23**

Appendix A Glossary of Acronyms **24**

Appendix B Evaluated Hardware Components **25**

Appendix C Evaluated Software Components **26**

EXECUTIVE SUMMARY

The National Security Agency (NSA) / National Computer Security Center (NCSC) examined the security protection mechanisms provided by ALC's Tigersafe. Tigersafe is a subsystem, not a complete trusted computer system. It was therefore evaluated against the *Computer Security Subsystem Interpretation* (CSSI) of the *Trusted Computer System Evaluation Criteria* (TCSEC). The computer security features evaluated were Identification and Authentication (I&A), and Object Reuse (OR). Tigersafe does not provide complete Discretionary Access Control (DAC) or Audit features. Therefore, those features were not evaluated.

The evaluation team determined that the highest rating at which Tigersafe satisfies the I&A and OR requirements of the CSSI is class D. The D rating in the evaluated features of I&A and OR resulted from Tigersafe's inability to meet all assurance and documentation requirements specified by the CSSI.

To obtain the level of trust described in this report, Tigersafe must be configured in accordance with the Trusted Facility Manual, or it's equivalent, and properly administered. There are some programs and utilities that should not reside on the IBM PC/XT/AT. These include the following: DOS system files, programming languages, compilers, debuggers, Tigersafe's utilities, and other application programs. Since Tigersafe only provides access control to it's own utilities, those other files and programs which should be controlled must be deleted from the system.

Subsystems are intended to add a level of assurance to an automatic data processing (ADP) system that has limited or ineffective security mechanisms. Subsystems are not intended to protect any information on an ADP system which processes classified information because subsystems may not be capable of maintaining the integrity of classified information. Subsystems should not be added to an ADP system for the sole purpose of processing classified or sensitive information.

Introduction

In May 1989, the evaluation team began a product evaluation of ALC's Tigersafe as supplied for the IBM PC/XT/AT Personal Computer. The objective of this evaluation was to rate Tigersafe against the *Computer Security Subsystem Interpretation* (CSSI) of the *Trusted Computer System Evaluation Criteria* (TCSEC) and to place it on the Evaluated Products List (EPL) with a rating for each of Tigersafe's evaluated features. This report documents the results of the evaluation. This evaluation applies to Tigersafe version 3.03.1 available from ALC Incorporated of Coronado, California.

Material for this report was gathered by the evaluation team through documentation, interaction with company representatives, and through the use of Tigersafe.

Evaluation Process Background

The National Computer Security Center (NCSC), located within the National Security Agency (NSA), was created to improve the state of computer security in computer systems processing information that is vital to the owners of that information. The Center fulfills its mission by promoting the development and implementation of trust technology and encouraging the widespread availability and use of trusted computer security products. Through the Trusted Product Evaluation Program (TPEP), the Center works with the manufacturers of hardware and software products to implement and make available to the public technically sound computer security solutions. Under this program, the Trusted Product and Network Security Evaluations Division evaluates the technical protection capabilities of computer security products against well-defined published evaluation criteria.

The product evaluation process culminates in the publication of a Final Evaluation Report, of which this document is an example. The Final Evaluation Report describes the product and assigns it a rating that denotes a specific level of trust. The assigned rating is independent of any consideration of overall system performance, potential applications, or particular processing environment. Rated products are listed on the Evaluated Products List (EPL), the aim of which is to provide ADP system developers, managers, and users an authoritative evaluation of a product's suitability for use in processing important information.

Subsystem Evaluation Program

The NCSC has recognized a need for guidance on, and evaluation of, computer security products that do not meet all of the feature, architecture, or assurance requirements of any one security class or level of the TCSEC. The NCSC has, therefore, established a Computer Security Subsystem Evaluation Program.

The goal of the Computer Security Subsystem Evaluation Program is to provide computer installation managers with information on subsystems that would be helpful in providing immediate computer security improvements to existing installations. Security Managers should note that subsystems are not capable of protecting information with sufficient assurance to maintain classified information on a system protected solely by security subsystems. Furthermore, subsystems may not be used to upgrade the protection offered by complete trusted systems for the sole purpose of adding the ability to store or process classified material. Subsystems may be added to other protection devices to provide another layer of security, but in no way may be used as justification for processing classified material.

Subsystems considered in the subsystem evaluation program are special purpose products that can be added to existing computer systems to increase some aspect of security and have the potential of meeting the needs of both civilian and government departments and agencies. For the most part, the scope of a computer security subsystem evaluation is limited to consideration of the subsystem itself, and does not address or attempt to rate the overall security of the processing environment.

To promote consistency in evaluations, subsystems' security mechanisms are assessed against the *Computer Security Subsystem Interpretation* (CSSI) of the *Trusted Computer System Evaluation Criteria.* Additionally, the evaluation team reviews the vendor's claims and documentation for obvious flaws which would violate the product's security features, and verifies, through functional testing, that the product performs as advertised. Upon completion, an evaluation report will assign a specific rating for each of the components of the subsystem and a summary of the evaluation report will be placed on the Evaluated Products List (EPL) which is maintained in the *Information Systems Security Products and Services Catalog.*

Document Organization

This report consists of four major chapters and three appendices. Chapter 1 is an introduction. Chapter 2 provides an overview of the subsystem hardware and software architecture. Chapter 3 provides a mapping between the requirements specified in the CSSI, and the Tigersafe's features that fulfill those Requirements. Chapter 4 is the evaluator's comments

about Tigersafe. The appendices consist of identification of specific hardware and software components to which this evaluation applies, and a glossary.

System Overview

Product History

ALC - The Stealth Group is a privately held company specializing in add-on security products for IBM Personal Computers and compatibles. They have been in business for approximately four years. ALC is currently marketing the TIGERSAFE Security and Audit Trail Tracking Subsystem in several packages offering various levels of security and features, and physical security options to prevent subverting the system by removal or physical modification. This evaluation is of the TIGERSAFE Model 3.03.1 installed to provide the maximum protection offered by the product.

Product Overview

The Tigersafe unit is a hardware board and software combination that performs Identification & Authentication and Object Reuse. The user plugs the hardware board into any 16 bit slot on the IBM PC/XT/AT, or compatible, and installs the software utilities with the provided installation program. The board asserts control, once loaded, by modifying the interrupt vector table. Tigersafe invokes its own code that controls the terminal and keyboard. The result is a password banner to which all users must correctly respond to access the utilities of the machine.

The software utilities provide functional control of the Tigersafe environment along with object reuse and minimal auditing. Tigersafe provides Master Administrator utilities that customize the Tigersafe system parameters, initialize users, and set passwords. Additionally, the Master Utilities manage user access to the hardware resources (hard disk, disk drive, parallel port, serial port, communications port, etc.), and configuration of the audit tool. Master Administrator utilities allow users to change their password, to customize the banner and to invoke the password banner during normal operation, all with authorization checking and optional audit.

The Tigersafe Model 3.03.1 was evaluated with multiple defined users in the configuration supplied for the IBM PC/XT/AT. It allows up to fifteen users to share a PC running PC-

DOS or MS-DOS version 2.1 and above. The product can also be used in a networked environment but was not evaluated in that configuration.

Security Relevant Portion (SRP)

The protection critical mechanism or the Security Relevant Portion (SRP) of Tigersafe, consists of its hardware and software capabilities. A description of these mechanisms and their security relevant roles are described in the following two sections.

Hardware Architecture

The hardware base of Tigersafe consists of a small, half-height circuit card, with four integrated circuits (IC) and supporting circuitry. The circuit card is available in several versions using both 2K and 8K Random Access Memory (RAM) chips. This evaluation only applies to the 8K circuit card. The four IC's are a battery-backed RAM chip, two Programmable Array Logic chips (PALs), and an address chip. The RAM chip stores variables and audit data for Tigersafe's operation. The two PALs contain the code for Tigersafe's execution. The address chip ensures that the system will recognize a valid card when the processor polls its address.

When power is applied to the system, a value is put into the instruction register which causes a jump to the location of the machine's boot procedure in Read Only Memory (ROM). This ROM code:

1. Runs a reliability test of chips on the board.
2. Tests the extent of memory and the physical environment.
3. Fills in the Interrupt Vector Table in low memory.
4. Checks for optional equipment by polling the card slots.

This polling is done by scanning memory in two kilobyte blocks, looking for additional devices on the bus. After a positive response, the CPU examines the first two bytes on Tigersafe's card to determine if it is a valid RAM card. If the RAM card is valid, the CPU reads the third byte for a size identifier. The CPU then performs a CRC check to verify that the code within Tigersafe is unchanged. If the checksum is valid, the CPU places Tigersafe's next byte into the instruction register. This marks the change of control from the computer's ROM boot sequence to Tigersafe's board.

The program then reserves the top one kilobyte of memory for Tigersafe's own use by modifying a value stored in the BIOS Data Area. Tigersafe decrements the value by one kilobyte, making DOS think it has, for example, only 639 kilobytes instead of 640 kilobytes. Having made this change, Tigersafe relocates some of the code from its own ROM into high memory. Tigersafe then replaces several interrupt vectors in the DOS low memory table so that the 8259 chip, which prioritizes all interrupts, will call this code.

The alteration of the vector table allows Tigersafe to front-end a number of ROM-BIOS routines. Part of the one kilobyte of reserved system memory is used by the DEVTRACK program (see page 6, "Software Architecture") to organize data structures so that it can intercept the DOS software interrupts for I/O operations. This allows Tigersafe to control whether individual users get access to hard drives, floppies, printers and com or serial ports. Tigersafe moves code that implements object reuse to this high memory area. After all the has been moved, Tigersafe checks the "Illegal Access" data table in its RAM data area to determine if the last time the PC was turned on, an illegal access was attempted. If so, a warning is printed to the screen and execution continues to the last step.

The last step is to display the entry screen and open up the keyboard to wait for a user password. Tigersafe's code is still in control and waiting for password entry. The key strokes for the password are encrypted when received and stored in a temporary buffer. When the return key is pressed, the temporary buffer is compared to the value stored in Tigersafe's RAM. If a match is found, Tigersafe examines its own data areas to see if *user identification* is enabled (see page 10 "Identification and Authentication"). If not, control is passed back to the CPU to finish its boot sequence. If enabled, it is checked before completing the boot process.

Software Architecture

This section describes the software components of Tigersafe's SRP. The software architecture of Tigersafe is a combination of software, firmware, and utility support programs. Security relevant actions are all done by firmware contained on the Tigersafe card. All administration and configuration actions are done through the utility programs. These programs are used by one of the three types of administrators configurable by Tigersafe. These administrators are able to gain access to the computer system, application programs, files, and Tigersafe utilities. The three administrators: The Master Security Administrator (MSA), the Department Level Administrator (DLA), and the end user, should be assigned to the individuals who have the specific responsibility for security of the computer workstations.

Tigersafe Utilities

Tigersafe can be installed to provide three levels of security. The administrator determines which level of security meets the needs of his organization by answering a questionnaire provided with the Tigersafe unit. Level Three installation provides the highest level of Tigersafe security feature capabilities and is the installation level used for this evaluation. Specifying the desired installation level determines which programs on the distribution floppy disk will be copied by installation command files. At Level Three, all program files are copied.

The utility TSMEMORY must be used prior to the Tigersafe card installation to check for any memory (ROM and RAM) addressing conflicts with existing add-on boards. TSMEMORY will alert the administrator if any adapter boards or drivers are in conflict with the Tigersafe addressing requirements.

The DEVTRACK program performs most of Tigersafe's security relevant functions. DEVTRACK intercepts DOS service requests and determines if they have an impact on Tigersafe programs or are requesting the use of a device. If the request is for a device, DEVTRACK compares the request to a master table of authorizations for the user. If the device is protected by DEVTRACK, or the user does not have the correct authorizations, the request will be either refused or ignored. Otherwise, the DEVTRACK program passes control directly to the DOS routine without any further intervention. During this processing, DEVTRACK logs the application program, file usage and system access events to their respective hard disk drive audit trails. DEVTRACK is also responsible for performing object reuse on deleted files. If enabled, DEVTRACK will overwrite the sectors of deleted files with alternating ones and zeroes.

The HWCONFIG utility must be used by the administrator to perform several hardware functions:

- Enable/disable CMOS verification at bootup.
- Enable/disable RAM overwrite with 0's each time the LOCK utility is used.
- Enable/disable system devices (floppy disk drives, hard disk drives, serial (COM 1-4) ports, and parallel (LPT 1-4) ports).
- Enable/disable secure file deletion to overwrite deleted files with 0's and 1's (Tigersafeoverwrites full clusters in case a file is less than 512 bytes).
- Enable/disable the keyboard and floppy drive during system booting.
- Display the Tigersafe hardware security configuration status.

- Display the Tigersafe serial number and audit file names.

The SECURITY utility, used by the administrator, sets up the passwords and identifications for up to 15 End Users. These User IDs and passwords are used by the I&A mechanism to validate users and to determine whether a user may access the floppy drive, hard disk, serial ports, and parallel ports. The SECURITY utility can also, optionally, prevent any duplicate End User passwords, define the maximum length of time an End User's password is valid and allow End Users to change their own passwords.

The LOCK utility is used by all users to return the PC to the initial logon screen. If used in conjunction with the SIGNOFF password, Tigersafe will overwrite extended/expanded memory and the 640K normal RAM memory with all 1's. The LOCK utility will check the computer's 50 byte CMOS setup data against a copy of the setup data stored on the Tigersafe board. If the CMOS data has changed, the PC will not accept any further keyboard input, logs the violation in the audit trail, and prints a warning to the screen stating that the CMOS memory has been modified. Tigersafe's SIGNOFF utility allows the administrator to set the password used in conjunction with the LOCK utility to clear the PC's RAM memory.

The DELAY utility is used by the system administrator to configure the maximum number of illegal password entry attempts. Once the threshold is reached, the PC's keyboard is locked out, the screen is cleared, and the violation is logged with the date and time. The PC will have to be rebooted before any user can log in again. The DELAY utility also allows the administrator to set the amount of time that the PC may remain powered up and idle in the LOCK screen. When the time limit is reached, the DELAY utility will clear all RAM memory, lock out the keyboard, and clear the screen. The timed lockup feature is only effective from the LOCK screen.

The CLOCK utility is used by the system administrator to link the computer's internal clock with the audit trails to log the date and time of events. This link is in the form of a clock driver chosen from a list of computer manufacturers and types. The installer specifies the manufacturer or model of the machine and the utility installs the proper driver software and links it to the audit programs. This should not be confused with the DOS time function, used to set the system clock, which has been protected to prevent altering the input to the audit trails. On protected systems the system clock can only be set by the administrators from the ROM Monitor utility.

Tigersafe's AUDIT utility allows the administrator to clear or display the four audit trail reports. The four reports are from the internal RAM-based session access log and the disk-based session access, program usage, and file usage logs, which are stored in ASCII format and accessible to all users. The audit trail reports can be viewed on screen or sent to a printer. The AUDITFN utility allows the administrator to enable any or all of the auditing functions and specify where to store the log files.

The administrator may change the Master Keycode, which is used to authenticate an administrator, by using the KEYCODE utility. The PASSWORD utility is used by the administrator to change the Master Password. The administrator may also enable the password option in the SECURITY utility to allow any users to use the PASSWORD utility to change their own passwords. When users are permitted to change their own passwords, the PASSWORD utility accepts user passwords and changes the password that is given for access.

SRP Protected Resources

This section describes the subjects and objects that Tigersafe mediates access between.

Subjects

The subjects are those processes and Tigersafe utilities that act on behalf of the system's users. A process is the abstraction of tasks which comprise an executing program. It consists of the current value of the program counter, registers, and associated variables. On a PC running DOS, all user processes execute in one mode. There is no memory separation for processes, nor is there a supervisor state or kernel to protect the operating system from user processes.

Objects

Tigersafe's protected objects are the following:

The named objects:

- Floppy Disk Drives
- Serial Ports
- Parallel Ports
- Addressable RAM memory
- CMOS memory - The first 50 bytes of battery back-up memory
- The Tigersafe DEVTRACK program

- The Tigersafe audit data files

The storage objects:

- Files
- CMOS Memory
- Memory - including extended/expanded memory

SRP Protection Mechanisms

This section describes Tigersafe's I&A and OR mechanisms.

Identification and Authentication

Once the Tigersafe boot sequence is complete, the user is presented with a logon screen requesting a password. The password may be six to twelve characters long and is controlled by the administrator. If *user identification* is enabled, and a password is successfully entered, the user's two character identifier is requested. The user identifier is defined by Tigersafe in a predictable sequence and cannot be changed. When the logon process is completed, the system will complete its boot process and leave the user at the DOS prompt. If the logon process is not successfully completed within the number of attempts selected by the administrator, the system will lock up, an entry will be made in the session access audit log, and the system must be rebooted by recycling power.

Tigersafe has the capability to record system access events. Auditable events are logon, logoff, or failed logon. Audit information is available in the Tigersafe Access Log.

Tigersafe allows up to fifteen users, including two administrators. To act with administrator privilege, one must use the Tigersafe utilities which require the Master Password plus a six to twelve character password, referred to as a keycode, for access. If one initially logged in using the Master Password, it would only be necessary to repeat it and the Keycode for access to the utilities, thus only passing two levels of security. After completing that process, the SECURITY utility provides the password configuration menu.

The configuration menu provides the following functions:

1. Enable user ID authentication.

2. Allows the MSA to force unique passwords.
3. Creation and editing of user passwords.
4. Password date control.
5. Definition of expiration times on user accounts.
6. Selection and editing of hardware access for users.

Object Reuse

Tigersafe provides object reuse on the storage objects as noted on page 9. This feature is activated by the administrator by initiating the "file overwrite", "CMOS clear", or "memory clear" options in the HWCONFIG utility. Once enabled, object reuse is provide in the following manner:

- File Overwrite - When the DOS ERASE or DELETE command is issued and this option is enabled, the disk sectors occupied by the designated file(s) will be overwritten. The administrator has the capability to specify how many times the sectors are to be overwritten and if they are to be overwritten with alternating ones and zeros.
- CMOS Clear - During logon, this option compares the first 50 bytes of memory to an internal buffer. CMOS memory is then overwritten with the buffer contents. If they differ, a warning message is displayed on the screen.
- Memory Clear - During logout, this option clears main memory, extended memory, and expanded memory.

Evaluation as a Subsystem

This chapter presents the CSSI requirements (and interpretations) for the features that were evaluated. The computer security features that were evaluated for the Tigersafe product are Identification and Authentication (I&A) and Object Reuse (OR). For each feature, this chapter states the requirements, describes Tigersafe's efforts to meet those requirements, and concludes with a statement as to the level of requirements that have been satisfied. This pattern is continued for each of the CSSI requirements for assurance and documentation. Finally, a rating assignment section (see page 22 "Rating Assignment") describes how the various individual ratings for features, assurances, and documentation combine to form a composite rating for each evaluated feature.

Features

Identification and Authentication

Requirement

The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual ADP system user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.

Interpretation

- D1:

The I&A subsystem shall require users to identify themselves to it before beginning to perform any other actions that the system is expected to mediate. Furthermore, the I&A

subsystem shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The I&A subsystem shall protect authentication data so that it cannot be accessed by any unauthorized user.

The I&A subsystem shall, at a minimum, identify and authenticate system users. At I&A/D1, users need not be individually identified.

- D2:

The following interpretations, in addition to those interpretations for I&A/D1, shall be satisfied at the I&A/D2 Class.

In the TCSEC quote, "TCB" is interpreted to mean "I&A subsystem." The I&A subsystem shall pass the protected system a unique identifier for each individual.

The I&A subsystem shall be able to identify each individual user. This includes the ability to identify individual members within an authorized user group and the ability to identify specific system users such as operators, system administrators, etc.

The I&A subsystem shall provide for the audit logging of security relevant I&A events. For I&A, the origin of the request (e.g. terminal ID, etc.), the date and time of the event, user ID (to the extent recorded), type of event, and the success or failure of the event shall be recorded. The I&A subsystem may meet this requirement either through its own auditing mechanism or by providing an interface for passing the necessary data to another auditing mechanism.

Applicable Features

Tigersafe requires that all users login through the login screen before taking any other actions. There are no apparent ways to circumvent this requirement. The passwords are sufficient to identify and authenticate users and administrators. Authentication data is stored in the isolated domain of the Tigersafe RAM and is not accessible to either authorized or unauthorized users. Tigersafe also provides for the auditing of security relevant I&A events.

Conclusion

Tigersafe satisfies the D2 feature requirement for I&A.

Object Reuse

Requirement

All authorizations to the information contained within a storage object shall be revoked prior to initial assignment, allocation or reallocation to a subject from the TCB's pool of unused storage objects. No information, including encrypted representations of information, produced by a prior subject's actions is to be available to any subject that obtains access to an object that has been released back to the system.

Interpretation

- D2:

In the TCSEC quote, "TCB" is interpreted to mean "protected system". Otherwise, this requirement applies as stated. The object reuse subsystem shall perform its function for all storage objects on the protected system that are accessible to users.

Applicable Features

Tigersafe overwrote all user accessible storage objects and there are no obvious ways to circumvent the mechanism. It must be noted that there are multiple options which must be activated to have an effective OR subsystem:

- RAM clear - extended/expanded memory.
- RAM clear - lower 640K memory.
- Enable secure file deletion.
- CMOS verification.

Conclusion

Tigersafe satisfies the D2 feature requirement for object reuse.

Assurances

System Architecture

Requirement

The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). Resources controlled by the TCB may be a defined subset of the subjects and objects in the ADP system.

Interpretation

- D1:

This requirement applies to all subsystems evaluated at all classes, regardless of the function(s) they perform. There are two specific elements of this requirement: Execution Domain Protection and Defined Subsets.

3.1.1.1 Execution Domain Protection

Protection of the subsystem's mechanism and data from external interference or tampering must be provided. The code and data of the subsystem may be protected through physical protection (e.g., by the subsystems dedicated hardware base) or by logical isolation (e.g., using the protected system's domain mechanism).

3.1.1.2 Defined Subsets

I&A subsystems, when used for the system's I&A, define the subset of subjects under the control of the system's TCB.

DAC subsystems may protect a subset of the total collection of objects on the protected system.

Applicable Features

Although Tigersafe's board isolates its I&A code and data, it does not maintain a domain for execution of the remaining parts of the SRP. Therefore, these parts are not protected from external modification. The controlled objects are defined on page 9, other objects on the PC are accessible and not protected.

Conclusion

Tigersafe does not satisfy the D1 system architecture requirement.

System Integrity

Requirement

Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

Interpretation

- D1:

In the TCSEC quote, "TCB" is interpreted to mean "subsystem".

This requirement applies to all subsystems evaluated at any class, regardless of the functions they perform.

Applicable Features

Tigersafe automatically performs a CRC check of the firmware and data structures located on its card when the PC is powered on. Tigersafe does not provide any diagnostics for the hardware or software components of its SRP.

Conclusion

Tigersafe does not satisfy the D1 system integrity requirement.

Security Testing

Requirement

The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. Testing shall be done to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms of the TCB.

Interpretation

- D1:

This requirement applies to all subsystems evaluated at any class, regardless of the function(s) they perform. In the TCSEC quote, "TCB" is interpreted to mean "subsystem".

The subsystem's Security Relevant Portion (SRP) shall be tested and found to work as claimed in the subsystem's documentation. The addition of a subsystem to a protected system shall not cause obvious flaws to the resulting system.

Test results shall show that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the subsystem's SRP.

Applicable Features

The evaluation team tested Tigersafe in two phases, the first focusing on functional testing, and then a second phase of security testing. Tigersafe was installed to provide the maximum of three levels of security available with the product. The functional testing phase concentrated on providing the team assurance that the product was installed properly and functioned consistently with the instructions provided. The security testing phase focuses on determining if there are any apparent ways to bypass or defeat the security mechanisms.

Functional testing is performed on the system as it may be installed in the field, using

DOS and any application programs that are not specifically forbidden by the instructions. All optional security features were turned on and several "accounts" were created for each member of the evaluation team. The system works as documented. Once an "account" is opened by entering the initial password at the SECURITY menu, it can only be changed and not deleted. The four audit logs are protected from modification and deletion by being set read-only but are viewable by all using either DOS or word processors. The Tigersafe utilities are protected from execution but are subject to deletion and spoofing by unsophisticated users.

The second phase of testing, security testing, consisted of exercising the system and looking for obvious flaws that would bypass or defeat the Tigersafe's protection mechanisms. Application programs, debuggers, utilities, and some locally written programs using both DOS and BIOS features were used. The team was not able to alter or bypass the authentication data on the circuit card itself or the I&A mechanism. However, Tigersafe is vulnerable to an insider attack. Introducing such programs to a protected system may require a significant amount of work, depending on how well the system is managed, but once on the system, Tigersafe is not able to protect itself or system resources. Manipulating audit data and other disk based data structures such as the file containing password expiration dates was a simple matter using either DOS or word processors. While manipulating the audit mechanism, the link to the clock was broken and the system continued to log invalid data without noting errors. Team members were able to change Tigersafe data in reserved memory using readily availably utilities. As testing progressed, operation of the Tigersafe utilities became very unpredictable and it was necessary to frequently reboot the system because the utilities would not exit properly.

Conclusion

Tigersafe does not satisfy the D1 security testing requirment.

Documentation

Security Features User's Guide

Requirement

A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one

another.

Interpretation

- D1

All subsystems shall meet this requirement in that they shall describe the protection mechanisms provided by the subsystem.

Applicable Features

A Security Features User's Guide was not provided with Tigersafe.

Conclusion

Tigersafe does not satisfy the D1 security features users guide requirement.

Trusted Facility Manual

Requirement

A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility.

Interpretation

- D1:

This requirement applies to all subsystems in that the manual shall present cautions about functions and privileges provided by the subsystem. Further, this manual shall present specific and precise direction for effectively integrating the subsystem into the overall system.

Applicable Features

Two Tigersafe manuals describe the installation and use of the utilities. These manuals focus upon the administrative procedures needed to execute these utilities, but do not present all of the cautions and warnings needed to control the facility.

Conclusion

Tigersafe does not satisfy the D1 Trusted Facility Manual requirement.

Test Documentation

Requirement

The system developer shall provide to the evaluators a document that describes the test plan, test procedures that show how the security mechanisms were tested, and results of the security mechanisms' functional testing.

Interpretation

- D1:

The document shall explain the exact configuration used for security testing. All mechanisms supplying the required supporting functions shall be identified. All interfaces between the subsystem being tested, the protected system, and other subsystems shall be described.

Applicable Features

ALC supplied test documentation showing the procedures and results of product installation and operation of some utilities. However, this documentation did not describe how the security mechanisms were tested nor the results of functional testing.

Conclusion

Tigersafe does not satisfy the D1 Testing Documentation requirement.

Design Documentation

Requirement

Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. If the TCB is composed of distinct modules, the interfaces between these modules shall be described.

Interpretation

- D1:

This requirement applies directly to all subsystems. Specifically, the design document shall state what types of threats the subsystem is designed to protect against (e.g., casual browsing, determined attacks, accidents). This documentation shall show how the protection philosophy is translated into the subsystem's SRP. Design documentation shall also specify how the subsystem is to interact with the protected system and other subsystems to provide a complete computer security system. If the SRP is modularized, the interfaces between these modules shall be described.

Applicable Features

ALC failed to supply adequate design documentation.

Conclusion

Tigersafe does not satisfy the D1 Design Documentation requirement.

Rating Assignment

This section describes the composite rating and how it is determined. A composite rating is assigned to each evaluated feature and is based upon the individual ratings issued in Chapter 3. The individual ratings are the rating for each feature and ratings for assurance and documentation supporting that feature. The chart below shows a 'Y' for each assurance or documentation requirement that is sufficient to support the rating of each feature. An 'N' indicates that the assurance or documentation requirement is not sufficient. For features that have a rating of 'D', the assurances and documentation requirements are irrelevant, and are marked 'N/A'. Using the ratings attained in Section 3, the composite ratings for each of Tigersafe's features are derived as shown in the following table.

Evaluated Features	Feature Rating	Assurance			Documentation				Supporting Function	Composite Rating
		Arch.	Integrity	Testing	SFUG	TFM	Testing	Design		
I&A	D2	N	N	N	N	N	N	N	Audit [1]	D
OR	D2	N	N	N	N	N	N	N	none	D

The CSSI requires that subsystems have *supporting functions* because some features rely on one another (e.g. an auditing subsystem needs user identities from the I&A subsystem). The CSSI permits a subsystem to accomplish this by alternative methods:

- The supporting function is provided by another feature of the subsystem.
- The supporting function is provided within the feature even though it may duplicate an aspect of another feature.
- The supporting function is provided through an interface to other products

If the supporting function is integrated within the product, it must be at the same level as that of the feature to obtain the composite rating.

[1] Authentication data protected on Tigersafe board. Tigersafe provides sufficient audit capability to support I&A

Evaluator's Comments

The evaluation team feels that the Tigersafe provides additional security by use of the I&A mechanism that PC-DOS and MS-DOS clearly do not possess. The company is very responsive to user needs and all problems identified to the company were quickly resolved. The D rating resulted from a lack of attention to the assurance requirements. The vendor is currently working on both an SFUG and TFM to aid administrators and users in making more effective use of Tigersafe's security features.

The Tigersafe provides security features adequate for a benign environment but the design of the administrators interface can be difficult to use. Some functions are duplicated and related options are not grouped together, which adds unnecessary complexity to administering the system. For instance, four options in three menus must be set to have a fully effective object reuse subsystem, and, options in three menus must be used to set password expiration dates. Audit trails are composed of four separate reports with no audit reduction capability, making them difficult to collate.

While the documentation improved greatly during the course of the evaluation, it is not well structured and is difficult to understand. Some sections consist entirely of disconnected notes, in the style of a footnote, that are not related. For example, the team deleted AUTOEXEC.BAT during a test of protection mechanisms and Tigersafe worked as advertised, leaving us with a locked system. To recover from that, it was necessary to remove the Tigersafe, restore the file, then reinitialize and reinstall Tigersafe. Relying on the documentation, the team frequently had to guess as to which section or sections applied to the task that they were attempting to accomplish.

Glossary of Acronyms

ADP	Automatic Data Processing
BIOS	Basic Input-Output System
CMOS	Complementary Metal Oxide Semiconductor
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSSI	Computer Security Subsystem Interpretation
DLA	Department Level Administrator
DAC	Discretionary Access Control
DOS	Disk Operating System
EEPROM	Electrically Erasable and Programmable Read Only Memory
EPL	Evaluated Products List
IC	Integrated Circuit
ID	Identification
I&A	Identification and Authentication
MAC	Mandatory Access Control
MS-DOS	MicroSoft Disk Operating System
MSA	Master Security Administrator
NCSC	National Computer Security Center
OR	Object Reuse
PC	Personal Computer
PAL	Programmable Array Logic
RAM	Random Access Memory
ROM	Read Only Memory
SRP	Security Relevant Portion
TCB	Trusted Computing Base
TCSEC	Trusted Computer Security Evaluation Criteria
TFM	Trusted Facility Manual

Evaluated Hardware Components

This appendix lists the ALC marketing identification numbers for all hardware covered by this evaluation. This list is equivalent to the set of hardware officially supported by the evaluation. The primary requirement for hardware is that the hardware function properly. This was verified by the diagnostic tests performed. Those tests were repeated periodically to ensure that identified problems originated within the subsystem and not the system itself.

To operate in correspondence with the I&A and OR ratings, the security subsystem must contain the hardware components listed in this section.

The protected system covered by this evaluation is the IBM PC/XT/AT.

Evaluated Software Components

This section lists the programs that make up the various divisions of Tigersafe's software. Tigersafe is designed to run under revisions 2.1, 3.1, 3.2, 3.3, 4.0 of PC-DOS, MS-DOS or IBM/DOS, although the Tigersafe audit trails only function under DOS 3.0 and above.

Version 3.03.1 of the Tigersafe software was evaluated. The software was delivered on two 5 1/4" floppy diskettes. The software consisted of the files listed below plus eight .DRV driver files for the CLOCK utility:

- ANALYSIS.DOC
- AUDITFN.COM
- CHAPTER1.COM
- CHAPTER2.COM
- CLOCK.COM
- DELAY.COM
- DEVTRACK.COM
- HWCONFIG.COM
- KEYCODE.COM
- LOCK.COM
- MANDISK.DOC
- MONITOR.COM
- PASSWORD.COM
- SAFEINIT.COM
- SECURITY.COM
- SECURITY.DOC
- SIGN.COM
- SIGNOFF.COM

- TIGERSAF.BIN
- TSCRYPT.COM
- TSCRYPTE.COM
- TSINIT.COM
- TSINSTA2.COM
- TSINSTAE.COM
- TSINSTAL.COM

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION **UNCLASSIFIED**	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT **UNLIMITED DISTRIBUTION**
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) **CSC-EPL--SUM-89/006**	5. MONITORING ORGANIZATION REPORT NUMBER(S) **S235,425**
6a. NAME OF PERFORMING ORGANIZATION **National SecurityAgency** 6b. OFFICE SYMBOL (If applicable) **C71**	7a. NAME OF MONITORING ORGANIZATION **National Computer Security Center**
6c. ADDRESS (*City, State and ZIP Code*) **9800 Savage Road Ft. George G. Meade, MD 20755-6000**	7b. ADDRESS (*City, State and ZIP Code*) **9800 Savage Road Ft. George G. Meade, MD 20755-6000**
8a. NAME OF FUNDING/SPONSORING ORGANIZATION 8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (*City, State and ZIP Code*)	10. SOURCE OF FUNDING NOS PROGRAM ELEMENT NO / PROJECT NO / TASK NO / WORK UNIT NO
11. TITLE (*Include Security Classification*) **Final Evaluation Report ALC Group TIGERSAFE (IBM)**	
12. PERSONAL AUTHOR(S) Deborah M. Clawson; Michael J. Oehler; Shawn M. Rovansek	
13a. TYPE OF REPORT **Final**	13b. TIME COVERED FROM ____ TO ____
14. DATE OF REPORT (*Yr, Mo., Day*) **891001**	15. PAGE COUNT **27**
16. SUPPLEMENTARY NOTATION	

17. COSATI CODES			18. SUBJECT TERMS (*Continue on reverse if necessary and identify by block number*)
FIELD	GROUP	SUB GR	**NCSC, I&A, OR, ALC Group, TIGERSAFE, CSSI**

19. ABSTRACT (*Continue on reverse side if necessary and identify by block number*)

The ALC Group TIGERSAFE (IBM Version) has been evaluated by the National Computer Security Center (NCSC). The security features of TIGERSAFE were examined against the requirements specified by the *COMPUTER SECURITY SUBSYSTEM INTERPRETATION OF THE DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA (CSSI) dated 16 September 1988.* The NCSC evaluation team has determined that TIGERSAFE meets several of the requirements for I&A/D2. TIGERSAFE failed to satisfy the documentation requirements and therefore it has been determined that the highest class at which the TIGERSAFE satisfies all the specified requirements of the CSSI is class I&A/D and OR/D.

This report documents the findings of the evaluation.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT UNCLASSIFIED/UNLIMITED	21. ABSTRACT SECURITY CLASSIFICATION **UNCLASSIFIED**	
22a. NAME OF RESPONSIBLE INDIVIDUAL **PATRICIA L. MORENO**	22b. TELEPHONE NUMBER (*Include Area Code*) **(301)859-4458**	8b. OFFICE SYMBOL **C71**